Networking Essentials

• What are the advantages and disadvantages of computer networking?

Advantages:

- **Data Sharing**
  - Eliminates *sneakernet* (shoe-based network)
- **Hardware/Internet Access Sharing**
  - e.g., printer, scanner, etc.
  - Special hardware devices allow the bandwidth of the connection to be easily shared among various devices as permitted
- **Data Security and Management**
  - Centralize data on shared servers
- **Performance Enhancement and Balancing**
  - Distribute computational task to various nodes on the network

Disadvantages:

- **Additional Overhead Cost**
  - Requires additional network device(s) and software configuration
  - Administration cost for maintenance and management
- **Undesirable Sharing**
  - Malware can also be transferred within the network
- **Data Security Concerns**
  - Poorly secured network can put data at risk and expose to other potential problems such as unauthorized access and even hold hostage

• Understand that the internet is primarily a packet-switched network and the implications of this.
The network breaks up data into packets. No resources are reserved in the switches to make a decision on where to send the packet. The switch dynamically figures out where to send the packet. This is helpful in case a switch fails to work.

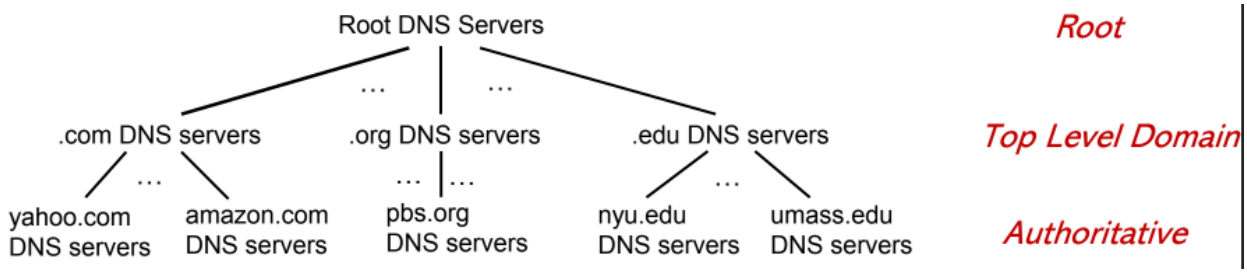
Resources are reserved in switches when the call is made in circuit switching. These resources are used by the switch to figure out where to send the packet. Once the call is resolved, the resources are restored.

• What are the network edge and network core?
Network edge is endsystems (e.g. servers, personal computers, etc.). The network core is a network of routers inter-connecting the end-systems (e.g. backbone, local area network (lan), internet service provider networks (ISPs), etc.).

• What is a threat model for the internet? Be able to explain and solve problems.
The threat model for the internet is threats to the internet.
Attacks to network edge: Automated malware that can travel through the systems, DDOS
Attacks to network core: Attackers can tap links to either monitor traffic or modify if, attackers can modify how the packets are routed in a specific way (changed the desired destination)

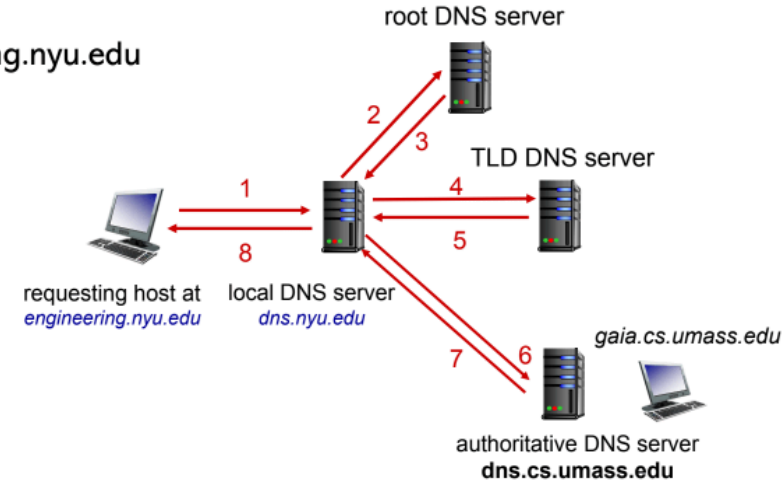
• What are the layers of the TCP/IP and OSI models and be able to explain what service/device/protocol belongs to what layer.
Application: supporting network applications
• FTP, SMTP, HTTP(S), DNS

Transport: process - process data transfer
• TCP, UDP
Network: routing of datagrams from source to destination
• IP, routing protocols
Link: data transfer between neighboring network elements
• Ethernet, 802.11 (WiFi), PPP
Physical: bits “on the wire”



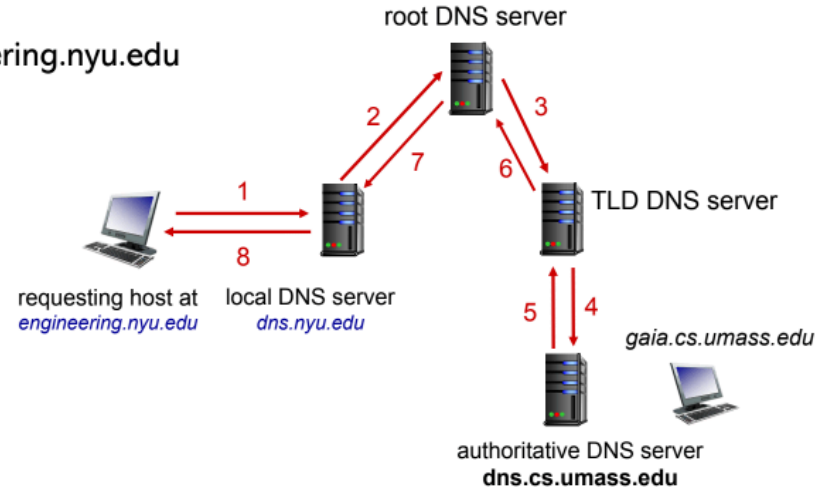
Example: host at engineering.nyu.edu wants IP address for gaia.cs.umass.edu

Iterated query:
- contacted server replies with name of server to contact
- “I don’t know this name, but ask this server”



Example: host at engineering.nyu.edu wants IP address for gaia.cs.umass.edu

Recursive query:
- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



presentation: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions

session: synchronization, checkpointing, recovery of data exchange
Please Do Not Teach Students Pointless Acronyms
physical data link network transport session presentation application

• What is the difference between the ethernet hub, ethernet switch, and ethernet repeater, and ethernet bridge? What is each device used for?
Ethernet Hub: Any system can talk to each other but only one at a time (if two systems talk to each other at the same time, there will be a collision)
• Collision domain (CSMA/CD)
• One-way traffic (half-duplex)
• No knowledge of addresses
• Messages are mirrored on all other ports

Ethernet Switch:
• Also referred to as a smart hub
• Learns MAC addresses to forward network traffic to a given port
• Allows simultaneous communication between connected devices (full duplex)

Ethernet Repeater: Amplifies signals, the signal will attenuate
• Also called signal extender
• Extend signal attenuation limit of a given media

Ethernet Bridge: Segment a network into multiple collision domains
• Has only two ports (only good for two computers to talk to each other)

• What are the LAN, WAN, and CAN?
Local Area Network (LAN):
• Network of computers connected relatively close together, i.e., room or building
Campus Area Network (CAN):
• Like LAN, but spans multiple buildings in the same location
Wide Area Network (WAN):
• Network that connects devices or other networks over a greater distance than LANs
• Distance between devices can be measured in miles.

• What is the difference between the ethernet router and ethernet firewall?
The ethernet firewall will allow or deny incoming or outgoing traffic based on the destination. Ethernet firewall has security built in by denying incoming or outgoing traffic based on the destination.

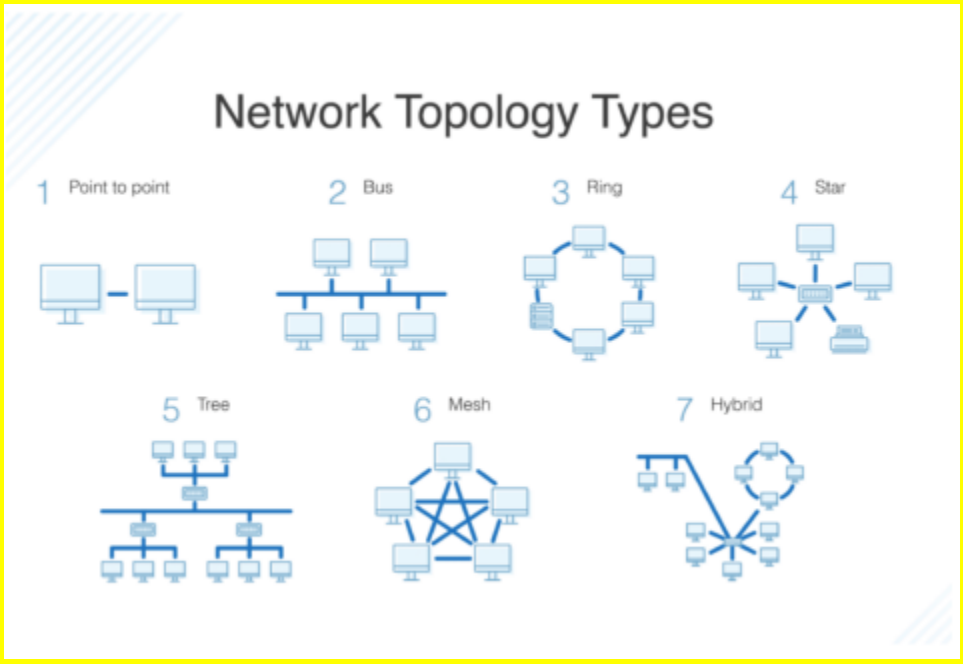
Ethernet Router: Forwards traffic to another network until it reaches the destination network
• Sometimes referred to as gateway

Router Firewall:

• Works as a packet filter router
• Forwards traffic to another network until it reaches the destination network
• Allow or deny incoming or outgoing traffic

• What is the difference between simplex, half-duplex, and full-duplex transmission modes?
Simplex: one-way communication (e.g. Airport Flight Information Display Systems, campus information display units)
Half-duplex: two-way communication, but not at the same time (e.g. hubs, walkie-talkies)
Full-duplex: two-way communication at the same time (e.g. bridges, switches, routers, cell phone)

• Be able to discuss the stability and security implications of each of the network topologies.



Bus: connects all the devices on a single shared channel
• Simple & cost - effective for small networks
• If shared channel fails, it brings down the entire network
• Only one node can send at any given time (Half - duplex)
• Not ideal for high volume network traffic
• If two systems are communicating, all other systems can understand what is being transmitted.

Ring topology: connects all the devices in a circle (or ring)
• Typically, a token is used to pick which node gets to start sending data.
• No packet collision: Data is passed from an adjacent node to the other neighbor node in a circular fashion until it reaches its destination.
• Easy node configuration
• Like the bus topology, only one node can send data at a time
• Failure of one node can bring down the entire network

• Failure in one connection will bring down the network
• Must interrupt the network to a add/remove network device

Star topology: laid out so every node in the network is directly connected to a central hub via coaxial, twisted-pair, or fiber-optic cable (most common network topology)
• Other network devices can be added or removed without interruption to the network operation
• Offers fault - tolerance: If an attached node goes down or a break on its network cable, it does not bring down the entire network
• Cost - effective (less connections needed) compared to other topologies such as Mesh or Full-Mesh
• If the central device goes down, all connected devices will lose connectivity
• Overhead to maintain the central device

Mesh topology: intricate and elaborate structure of point-to-point connections where the nodes are interconnected
• Provides more fault tolerance when one or more hosts/links fail but will not bring down the network
• Reliable to deliver data to destination in any available path
• Complex layout makes it harder to troubleshoot
• Costs the most of needed resources
• Labor - intensive setup

Ethernet Switching and VLANs

• At what layer do ethernet switches function?
Ethernet switches function on layer 2 or the data link layer.

• What is the difference between a managed and unmanaged switch?

• Understand that ethernet switches are transparent to hosts and are plug-and-play devices.
Switches are:
Transparent: hosts unaware of presence of switches
Plug-and-play, self-learning
No manual configuration needed

• Be able to explain how switches construct forwarding table and be able to solve problems similar to the assignment.
1. Take note of the source mac from sender
2. Check if destination is in the CAM table
3. Flood all systems to figure out which port the system is on
4. The system will respond and the switch will add it to the CAM table

• What is the difference between a switch and a router?
both are store-and-forward:
routers: network-layer devices (examine network - layer headers)
switches: link-layer devices (examine link-layer headers)
both have forwarding tables:
routers: compute tables using routing algorithms, IP addresses
switches: learn forwarding table using flooding, learning, MAC addresses

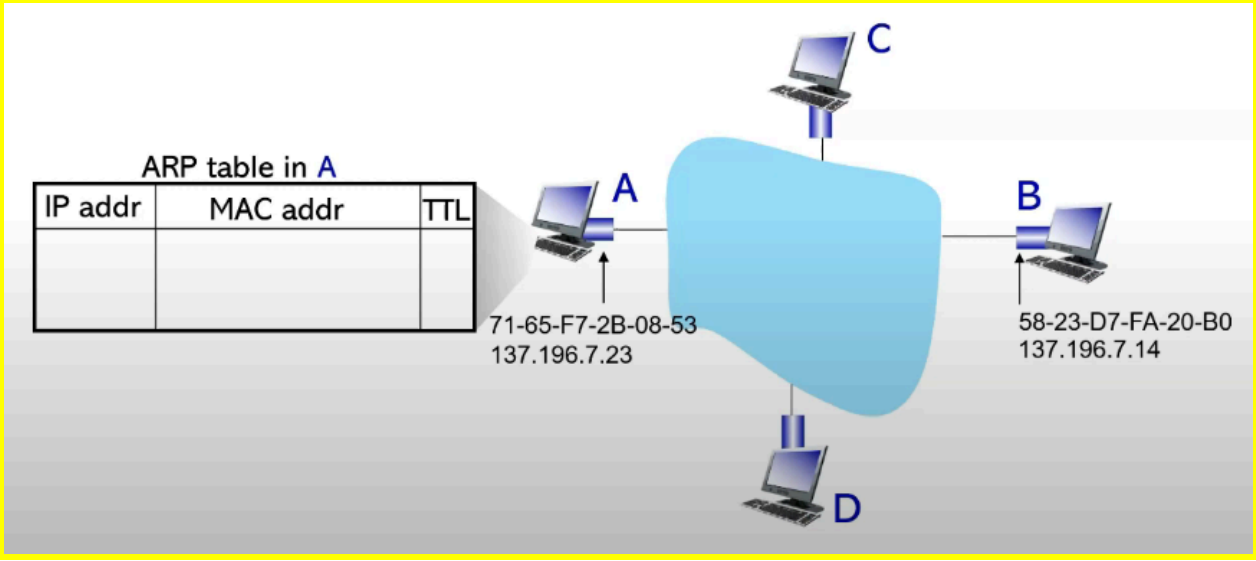
• What are the scalability and security issues involving large LANs?
All layer 2 broadcast traffic must cross the entire LAN.

• What are Virtual LANs (VLANs)? Be able to explain and solve problems.
VLANs are switch(es) supporting VLAN capabilities that can be configured to define multiple virtual LANS over single physical LAN infrastructure.

• What are security advantages of VLANs and how are VLANs used for network segmentation?
VLANs are able to separate ports into multiple switches. This way communication inside the switch would be separated.

ARP Poisoning Attacks

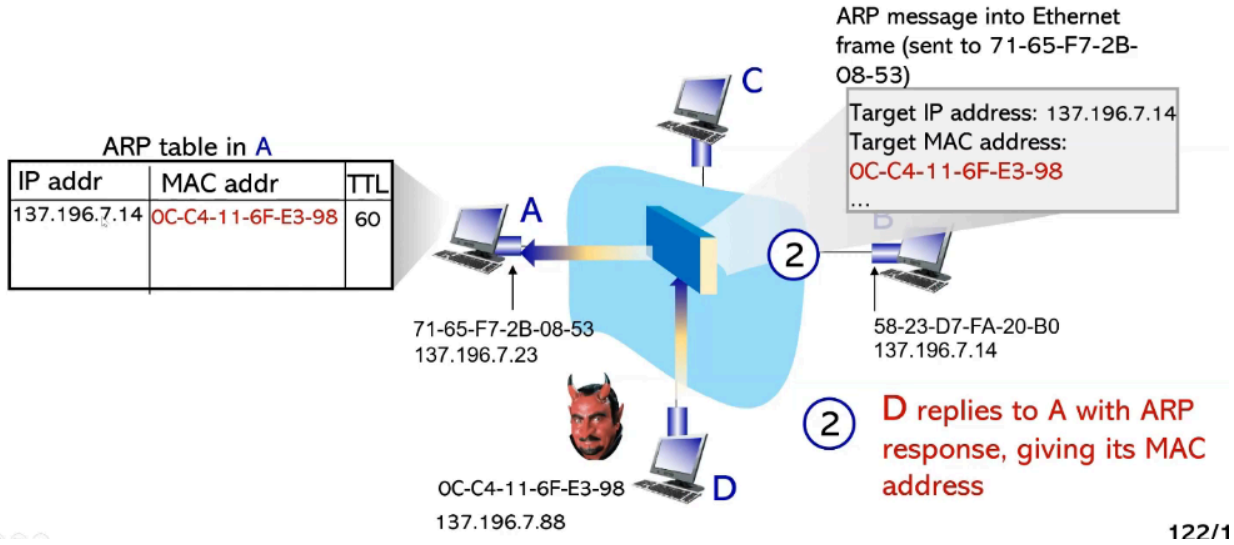
• What is the ARP protocol? Be able to explain and solve related problems.
The ARP protocol is “address resolution protocol”. ARP connects the link layer to the network layer. It helps connect the MAC address of the system to the IP address of a system we already know.



1. System A sends a broadcast containing B’s IP address
2. The query includes the source MAC, source IP, and target IP address
3. System B replies to A with ARP response, giving its MAC address

4. System A receives B's reply, adds B's entry into the local ARP table

• What is an ARP poisoning attack? Be able to explain how the attack is performed.
An ARP poisoning attack is when another system responds to the query sent by System A.



1. System A sends a broadcast containing B's IP address
2. The query includes the source MAC, source IP, and target IP address
3. System D replies to A with ARP response, giving its MAC address instead of System B
4. System A receives D's reply, adds D's entry into the local ARP table
5. Anything sent to System B will instead be sent to System D

• Be able to understand the output of the arp command and using it to identify signs of an ARP poisoning attack.
You can use the command "arp -n" to bring up the ARP table and see if any IP addresses are mapped to the same MAC address.

IP and Subnetting

• What is subnetting?
Subnet is a part of a larger network that has a specific range of IP addresses. You divide a network into multiple subnetworks by borrowing subnet mask host bits to be turned into network bits. Systems have to be on the same subnet to communicate.

• What are the practical applications of subnetting?
Some examples of subnets are:
• A LAN that connects the computers and devices in a certain department or floor of an organization
• A network that covers all the systems in a specific city or county
• A network that links all the systems in the same building or campus

• Know the structure of the IP address.
128.20.12.5
Network/sub Host
10000000.00010100.00001100.00000101
Network Address: 10000000.00010100.00000000.00000000
128.20.0.0/16
Host address: 00000000.00000000.00001100.00000101
0.0.12.5

Block size = How many IP addresses can we represent on the network = 2 ** 16

# of host addresses = the number of IP address that can be assigned to hosts (block size - 2)

Such IP address cannot be assigned to hosts
x.x.x.0 - used to represent network address
x.x.x.255 - used to represent a broadcast

192.168.2.0/24
11000000.10101000.00000010.00000000
We want to split it into 4 subnets.
How many bits do we need to represent 4 distinct network addresses?

$2^b = 4$
b = 2

11000000.10101000.00000010.00000000/26 = 192.168.2.0/26
11000000.10101000.00000010.01000000/26 = 192.168.2.64/26
11000000.10101000.00000010.10000000/26 = 192.168.2.128/26
11000000.10101000.00000010.11000000/26 = 192.168.2.192/26

192.168.2.0/24
11000000.10101000.00000010.00000000
We want to split it into 6 subnets.
How many bits do we need to represent 6 distinct network addresses?

$2^b = 6$
b = 3

$2^3 = 8$

11000000.10101000.00000010.00000000/27 = 192.168.2.0/27
11000000.10101000.00000010.00100000/27 = 192.168.2.32/27

11000000.10101000.00000010.01000000/27 = 192.168.2.64/27
11000000.10101000.00000010.01100000/27 = 192.168.2.96/27
11000000.10101000.00000010.10000000/27 = 192.168.2.128/27
11000000.10101000.00000010.11000000/26 = 192.168.2.192/27
11000000.10101000.00000010.11100000/26 = 192.168.2.224/27

Merge the following subnets into one network:

192.168.64.0/19(255.255.224.0)
192.168.96.0/19(255.255.224.0)
192.168.128.0/19(255.255.224.0)
192.168.160.0/19(255.255.224.0)
192.168.192.0/19(255.255.224.0)
192.168.224.0/19(255.255.224.0)

11000000.10101000.01000000.00000000/26
11000000.10101000.01100000.00000000/26
11000000.10101000.10000000.00000000/26
11000000.10101000.10100000.00000000/26
11000000.10101000.11100000.00000000/26

11000000.10101000.00000000.00000000/16
192.168.0.0/16

• What is classful addressing? Know the different network classes.
Classful addressing is a method of dividing the IP address space into different segments.

Class	Octet 1	Octet 2	Octet 3	Octet 4
A	Subnet	Host	Host	Host
B	Subnet	Subnet	Host	Host
C	Subnet	Subnet	Subnet	Host

– Example: Which class can support the greatest number of hosts?
Class A can support the greatest number of hosts since it has 3 octets to represent the host bits.

Class	Public Address Range	Private Address Range	# of Representable Subnets	# of Representable Hosts
A	1.0.0.0 – 127.0.0.0	10.0.0.0 – 10.255.255.255	126	16,777,214
B	128.0.0.0. – 191.255.0.0.	172.16.0.0 – 172.31.255.255	16,382	65,534
C	192.0.0.0 – 223.255.255.0	192.168.0.0 – 192.168.255.255	2,097,150	254

– Example: What class does the IP address 192.168.1.2 belong to?
Class C

– Example: What class does the IP address 128.56.6.8 belong to?
Class B

– Example: Consider a classful address of 128.80.2.5. What is the host and network portion?
128.80 2.5
Network/sub Host
10000000.01010000.00000010.00000101

• What are the disadvantages of classful addressing?
One disadvantage is that there is not much flexibility since you have to decide between /8, /16, or /24.

• What is Classless InterDomain Routing (CIDR)? How does it compare to classful routing?
Splits the IP address into two sections: the first specifies the network subnet address and second the address of the host on the network
▪ subnet portion of address of arbitrary length
▪ address format: a.b.c.d /x , where x is # bits in subnet portion of address

• Be able to identify the subnet and host parts of the CIDR address.
– Example: Consider address 128.20.12.5/16. What are the host and network portions of the address?

– Example: Consider address 192.168.6.7/24. What are the host and network portions of the address?

• Be able to translate between the dotted decimal notation and CIDR masks.
– Example: Consider address 124.12.42.3 and the subnet mask 255.255.252.0. What CIDR prefix is the mask equivalent to? What are the subnet and host portions of the address?

– Example: Consider address 137.151.45.6 and subnet mask of 255.255.0.0. What is the CIDR prefix is the mask equivalent to? What are the subnet and host portions?
/16

• Be able to break up networks into subnets.
– Example: Consider subnet 137.20.0.0/16. Split the network into 6 different subnets.

– Example: Consider subnet 128.34.128.0/17. Split the network into 3 different subnets.
• What is supernetting. Be able to understand and solve problems.

– Example: Consider subnets 192.168.12.0/24, 192.168.3.0/24, and 192.163.45.1/24. Merge them into a single subnet.

11000000.10101000.00001100.00000000
11000000.10101000.00000011.00000000
11000000.10100011.00101101.00000000

11000000.101000000.00000000.00000000 = 192.160.0.0/12
Get the largest common bits

– Example: Consider subnets 128.78.128.0/17 and 192.168.64.0/18. Merge them into a single subnet.

10000000.01001110.10000000.00000000
11000000.10101000.010000000.00000000

10000000.00000000.00000000.00000000 = 128.0.0.0/1

• What is the difference between static and dynamic IP address assignment?
Static Approach: the system is manually configured to use a specific IP
Dynamic Approach: DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
• can renew its lease on address in use
• allows reuse of addresses (only hold address while connected “on”)
• support for mobile users who want to join network (more shortly)

• What is Dynamic Host Configuration Protocol (DHCP)? Be able to discuss the steps.
host broadcasts “DHCP discover” msg [optional]
DHCP server responds with “DHCP offer” msg [optional]
host requests IP address: “DHCP request” msg
DHCP server sends address: “DHCP ack” msg

R1# interface FastEthernet 0/0 // Configure the interface FastEthernet 0/0
R1(config - if)# ip address 192.168.1.1 255.255.255.0 // Set the IP address
R1(config - if)#no shutdown // Activate the interface R1(config - if)
#end // Exit the current configuration mode
R1#configure terminal
R1(config)#service dhcp / / Let’s configure DHCP

R1(config)#ip dhcp excluded - address 192.168.1.1 192.168.1.99 // Do not assign these addresses
R1(config)#ip dhcp pool MYDHCPOOL // Create a pool of DHCP addresses called MYDHCPOOL
R1(dhcp - config)#network 192.168.1.0 255.255.255.0 // Grant addresses from this range
R1(dhcp - config)#lease 2 // Let the systems keep these addresses for 2 days
R1(dhcp - config)#default - router 192.168.1.1 // Local gateway router
R1(dhcp - config)#end // Exit configuration

• What are the different security attacks against DHCP?
A system could send tons of requests to the DHCP, eating up IP addresses in the pool. This system would need to use MAC spoofing.

• Be able to dynamically and statically configure IP addresses in Windows and Linux.

• What is the difference between the subnet mask and the wildcard mask?
You invert the bits of the subnet mask to get the wildcard mask.
Subnet mask: 1111111.1111111.1111111.00000000 = 255.255.255.0
Wildcard mask: 00000000.00000000.00000000.11111111 = 0.0.0.255

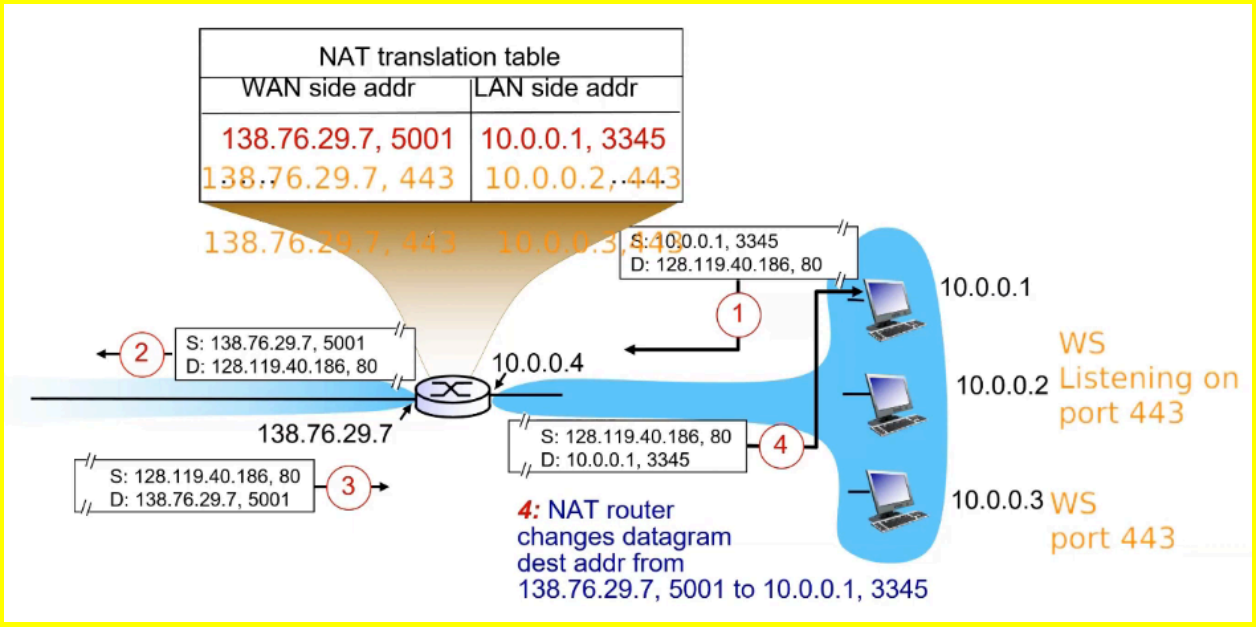
NAT

• Explain what NAT stands for and how it is used in networking. Give some examples of its practical applications and how to solve problems involving NAT.
NAT stands for network address translation. NAT hides multiple systems behind a single public IP address.

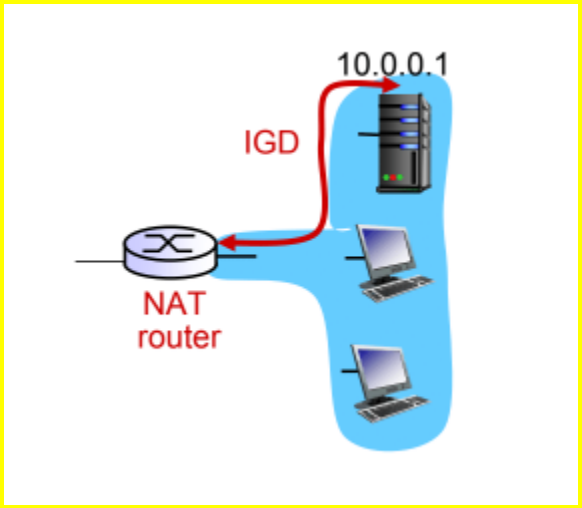
• How can NAT's be beneficial to security?
A NAT router will replace the source address and port number of every outgoing datagram with a NAT IP address and a different port number.

• Discuss the pros and cons of NAT for network performance, security, and scalability.
Pros:
Cons: Creates overhead and can be slow due to all the packet rewriting, Systems outside the NAT cannot connect to systems in the NAT
2^{16} port simultaneous sessions

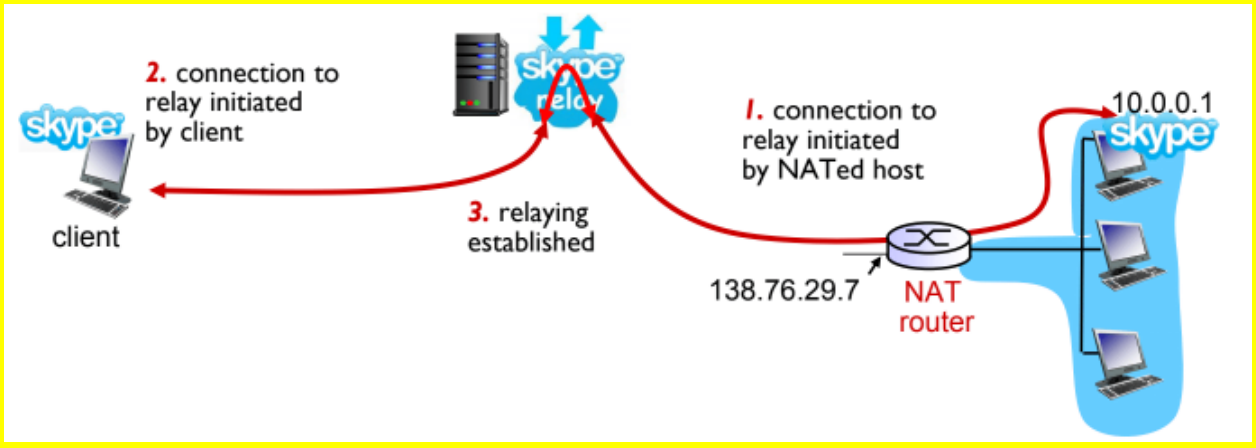
• Compare and contrast the different techniques for NAT traversal. How do they work and when are they used?
Port-forwarding: statically configure NAT to forward incoming connection requests at given port to server (Manually add a new entry to the NAT table)



Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol: Use an application such as IGD to add/remove entries to the NAT table (Port-forwarding but using a protocol)



Relaying: Relay bridges packets between two connections

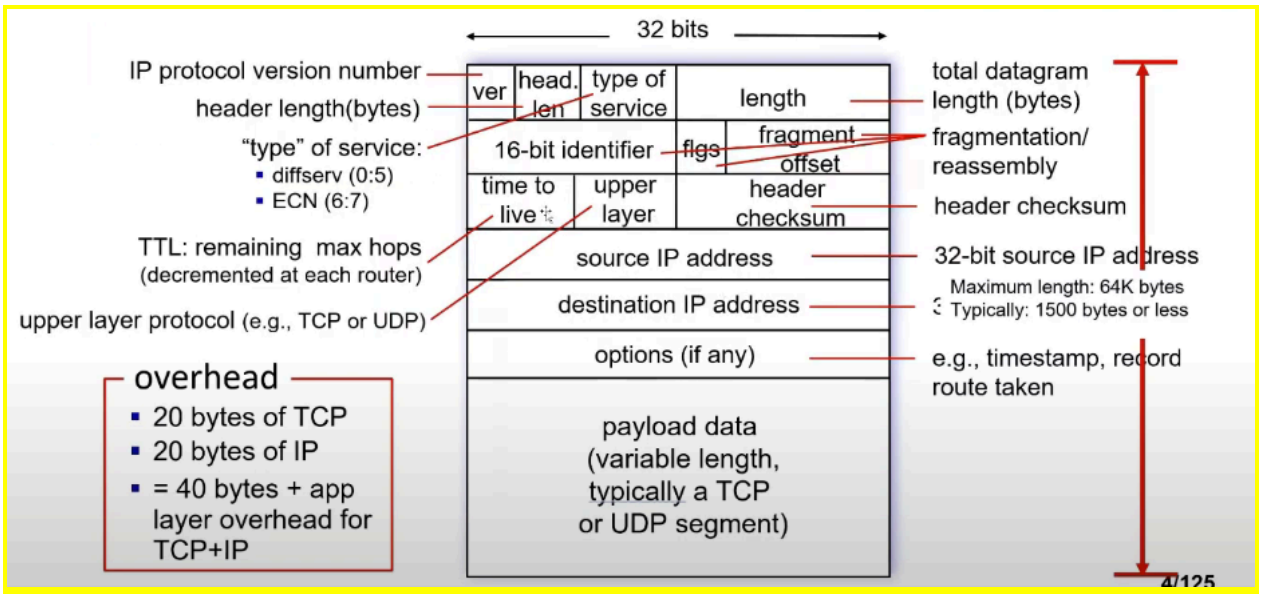


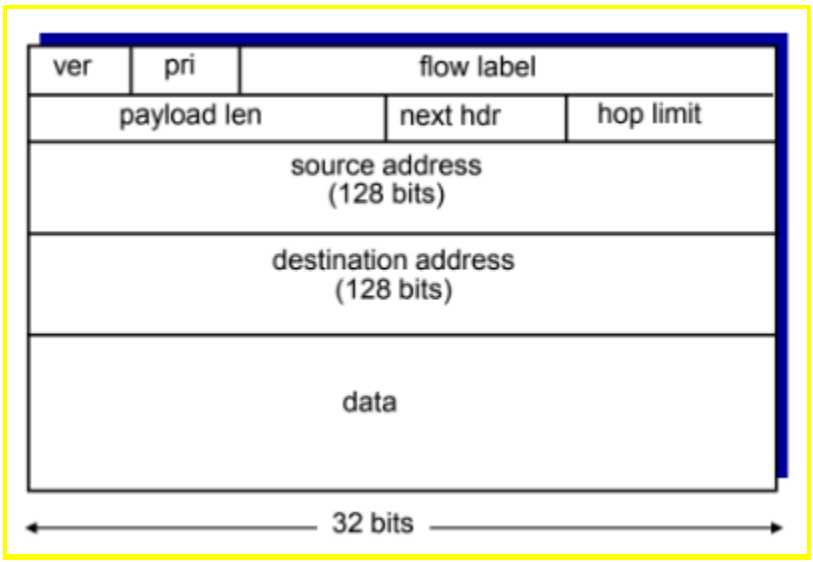
• Understand and be able to trace the process of packet transformation as the packet exits an internal NATed network and how the response from an external source is modified upon re-entry through NAT.

• Be able to configure NAT in a Cisco router. You will be given access to Cisco router documentation.

IPv6

• What is the difference between the IPv6 and IPv4 packet structure?
IPv4 packet header can vary. If the IPv4 packet header is too long, the packet can be fragmented. IPv6 headers are a fixed 40 bytes.





Version: Specifies whether this is an IPv4 or IPv6 address
Priority: identify priority among datagrams in flow
FlowLabel: identify datagrams in the same "flow." (concept of " flow " not well defined).
Next header: identify upper layer protocol for data
Hop limit: How many hops this packet can traverse before it gets dropped

• Why is IPv6 considered to be more efficient and secure than IPv4?
IPv6 uses a fixed header size which allows the packets to be more efficient. IPv4 packets also allow fragmentation.

• What is IPv6 tunneling and what is it used for?
IPv6 tunneling encapsulates an IPv6 packet inside an IPv4 packet. It adds an IPv4 header to the packet. This allows newer IPv6 routers to communicate with older IPv4 routers.

Routing Basics

• Be able to explain the basic process of how the router routes.
When a router receives a packet on one of the ports, it needs to decide to which port the packet should be forwarded to. Each router maintains a routing table that specifies on which port to forward the packet. The longest prefix match routing algorithm is one of the criteria used to determine the output port.

• Understand and be able to explain the longest common prefix routing and solve problems.
When a packet comes in, the router will look at the set of prefixes in its forwarding table. Whichever prefix has the longest match with the destination address, the router will output the packet to whichever port is associated with the prefix.

– Example: Consider a packet with the destination IP address of 128.34.23.29 and a router with the routing table below. To what port will the packet be forwarded to?

Prefix	Port
192.168.0.0/16	1
192.168.128.0/17	2
192.168.160.0/19	3
Default	4

192.168.0.0/16 = 11000000.10101000.xxxxxxxxx.xxxxxxxx 1
192.168.128.0/17 =11000000.10101000.1xxxxxxx.xxxxxxxx 2
192.168.160.0/19 =11000000.10101000.101xxxxx.xxxxxxxx 3
Default 4

128.34.23.29 = 10000000.00100010.00010111.00011101
Since none of these match any of these prefixes, the packet is outputted on port 4.

192.168.5.34 = 11000000.10101000.00100010.00000101
Since it best matches the first prefix, the packet is outputted on port 1.

192.168.128.45 = 11000000.10101000.1000000.00101101
Since it best matches the second prefix, the packet is outputted on port 2.

Nmap and Network Mapping

• What is network mapping and why is it important in security?
Network mapping is discovering and visualizing the devices, connections, and topology of a network including: Hosts, Ports, Services, Subnets, Protocols, Policies, Vulnerabilities. You are able to see all incoming and outcoming traffic of a device.

• Be able to use nmap to map out networks and read the nmap output. You will be given the nmap manual and you may use the nmap man page.
nmap <subnet>

```
root@UbuntuDockerGuest-3:~# nmap 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-24 06:15 UTC
Nmap scan report for ResearchBackend (192.168.122.1)
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:35:E8:21 (QEMU virtual NIC)

Nmap scan report for UbuntuDockerGuest-1 (192.168.122.153)
Host is up (0.00022s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 4A:14:67:4E:6F:50 (Unknown)

Nmap scan report for UbuntuDockerGuest-2 (192.168.122.184)
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 7A:39:2B:C4:A9:AB (Unknown)

Nmap scan report for UbuntuDockerGuest-3 (192.168.122.66)
Host is up (0.0000030s latency).
All 1000 scanned ports on UbuntuDockerGuest-3 (192.168.122.66) are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.49 seconds
root@UbuntuDockerGuest-3:~#
```

This command can be used to scan all open ports on the network.

• What is the difference between open, closed, filtered, and unfiltered ports?
Open: The application listening on the port is actively accepting TCP connections, UDP datagrams, or SCTP associations
• If you are a hacker or a penetration tester, this finding means that you can try to exploit the application running on the port to find an entry into the system
• If you are a defender and discover an open port that should not be there, the port should be closed (perhaps the application is a backdoor)

Closed: The port is accessible but has no application running on it
• Sometimes ports are put into this state to enable pinging or host discovery

• If you are the penetration tester, you may want to scan these ports again later to see if they open up

Filtered: Nmap was not able to probe the port because its probes were likely blocked by a firewall
• Firewalls can block access to certain ports on certain hosts to help frustrate attackers
• Sometimes firewall filters will respond with ICMP error messages, but most will usually drop the nmap probe

Unfiltered: Nmap cannot tell if the port is open or closed based on the probe response
• May need to use other scan types to find out. This means that the port is not blocked by a firewall or another device, but it does not reveal its state

• Know and be able to use the different modes of nmap.
-F: Performs a fast scan
-A: Does a deeper probe on the system (Scans the OS and other details)
-sA: Used to detect the firewall settings if the host has an active firewall
-sS: Stealth mode scan. Works by sending the TCP SYN packet to the port and sees if the SYNACK response is received. Generally slower and less aggressive than other scans.
-sP: Simply pings all of the systems in the specified range to help establish active servers
-D: A decoy scan. Will scan the host while making the target think that the scan is happening from different locations. Will make it difficult for the target to establish who is the actual scanner.

– Example: What will the following nmap command do nmap -sS 192.168.0.1 -p 1-2000
Scan IP address 192.168.0.1 in stealth mode scanning ports 1-2000

– Example: How to conduct a decoy scan of system 192.168.4.3 using systems 192.168.4.5 and 192.168.4.3 as decoys?
nmap -D 192.168.4.5, 192.168.4.3, ME 192.168.4.23

Cisco Router Basics

• What is the difference between the Cisco router's startup and running configurations? How to save the running configuration into start up configuration?
The running configuration is the current configuration in the router's volatile memory. The startup configuration is the configuration the router boots up on startup.

– Example: Consider a Cisco router with network interfaces FastEthernet0/0, FastEthernet0/1, and FastEthernet1/0. Configure the interfaces with IP addresses of 192.168.2.1, 192.168.3.1, and 192.168.4.1 all with the mask of of /24
R1#config t
R1(config)#interface f0/0

```
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shut
R1(config)#interface f1/1
R1(config-if)#ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#end
R1#show running-config
```